STATE OF ALABAMA

Information Technology Policy

Policy 620-03_Rev B: Authentication

OBJECTIVE:
Define the minimum requirements for authenticated access to State information systems.

SCOPE:
This policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

RESPONSIBILITIES:
Every user shall be assigned a unique user identification and authentication mechanism (e.g., user ID and password) so all activities on the network are traceable to a specific user.

At a minimum, users shall uniquely identify themselves to the system or network resource and verify that identity with at least one authentication factor.

Authentication factors include something a person knows (password, pass-phrase, PIN, etc.), something a person has (token, access card, etc.), or something a person is (biometric such as a fingerprint, retina scan, etc). Authentication factors may be required in any combination (i.e., multi-factor authentication).

Authentication factors must never be shared, cached, stored in any readable form, or kept in locations where unauthorized persons might discover them.

Information systems shall obscure feedback of authentication information during the authentication process.

Detailed authentication requirements shall be documented in applicable standards and procedures.

Users shall be provided guidance on protecting identifiers and the corresponding authentication mechanism.

ENFORCEMENT:
Refer to Information Technology Policy 600-00: Information Security.

Signed by Jim Burns, Chief Information Officer

DOCUMENT HISTORY:

Version	Release Date	Comments
Original	3/9/2006	
Rev A	1/12/2007	Added biometric policy and user guidance statements.
Rev B	10/28/2008	Added authenticator feedback requirement; moved biometric requirement to Standard 620-03S2: Authentication-Biometrics.